REMARKS

Claims 1-4, 6-12, 21-26, and 28-30 were pending in the patent application. By this amendment, Applicants have canceled Claim 26. The Examiner has rejected Claims 7-12 and 21-26 under 35 USC 112 as indefinite. Claims 7, 9, 10 and 12 have been amended in accordance with the Examiner' suggestion to now recite a removable security device installed therein. In addition, Claims 21-25 have been amended to properly depend from non-canceled claims and Claim 26 has been canceled. Applicants believe that the amendments address all of the 112 rejections. The Examiner has indicated that Claim 12 recites allowable subject matter and would be allowed if rewritten to overcome the objections discussed above. Claims 21 and 25 have been amended to depend from Claim 12 and are believed to be allowable as well.

Claims 1-4, 6-11, 21-26, and 28-30 have been rejected under 35 USC 103 as being unpatentable over the teachings of the Isikoff patent in view of Elledge and Kunert. Applicants respectfully assert that the remaining claims, Claims 1-4, 6-11, 21-25, and 28-30 are allowable over the cited art.

The present invention relates to a portable computer having a radio frequency identification chip (RFID chip) and a radio frequency antenna (RF antenna) security device incorporated therein. The computer apparatus and method provide for detection of removal of the RF antenna security device and denial of access to the computer if it is determined that removal of the RF antenna security device was unauthorized. Under the present invention, unlike the prior art, the security device can optionally be legitimately removed from the portable computer with authorization, and access to the computer will not be denied. The computer has a first storage area for storing data including an antenna history bit indicating whether a security device was ever attached to the computer. That storage area is capable of storing information received from an RF source even when the computer is not powered up. Moreover, the invention further provides for protection of that stored data (i.e., prohibiting access to change that stored data) so that an unauthorized user cannot alter the original stored information. Upon successive monitoring by the CPU, or powering up of the computer, the antenna history bit of the stored data is accessed to determine whether a security device was ever attached to the computer. Further,

it is dynamically determined if the security device is presently attached to the computer. If the security device is not presently attached, and removal was not legitimate (as determined, for example, by entry of an authorized password), access to the computer is denied. If, however, it is determined that removal of the security device was legitimate, access to the computer is permitted, and the authorization information is stored for future reference.

The Isikoff patent is directed to a computer antenna which is used both for communication and security. If the computer is stolen, the antenna signal can be traced to locate the computer. Isikoff provides for the antenna to be activated as a security device when unusual activity is detected. In addition, Isikoff mentions, although does not provide implementation details for, actuating internal security protocols, such as erasing the hard drive, in response to the unusual activity. Applicants respectfully assert, however, that Isikoff does not teach or suggest the invention as claimed.

Isikoff does not provide a first storage location, for storing at least an antenna history bit, even when the power is not turned on, wherein the stored data indicates whether an RF antenna security device was ever attached to the

computer. Isikoff does not teach or suggest that antenna history data be stored or accessed in order to verify whether an antenna should be connected. Rather, Isikoff detects a misentered password (Col. 9, lines 11-13) or may test circuitry wired to the antenna (Col. 4,, lines 43-44) in order to determine that the computer has been stolen or tampered with. Further, Isikoff does not provide any details regarding legitimate removal of, or disabling of, its antenna, use of a password to allow legitimate removal of its antenna, or storage of information regarding legitimate removal of its antenna. Isikoff expressly teaches that the antenna is integral to the computer unit and that any tampering is unauthorized. Finally, while Isikoff does suggest disabling some operation of the computer when tampering or removal is detected, Isikoff does not teach or suggest that access to the computer is prohibited unless the removal of the antenna is verified as appropriate (i.e., the antenna history bit indicates that no antenna was attached) or authorized (i.e., that removal was appropriate as verified through use of a password in conjunction with the antenna history bit). Since Isikoff's RF pager system is designed to transmit to outside receivers, Isikoff clearly does not teach or suggest that

its RF antenna communicates data to an internal RFID chip even when the computer is not powered on.

Applicants respectfully assert that neither the Elledge or Kunert patents teaches that which is missing from the Isikoff patent. The Elledge patent is cited for teaching an RFID in a laptop, with particular reference to the passage from Col. 7, lines 12-21. Elledge provides no teachings, however, of storing an antenna history bit which indicates that an RF antenna was once connected to the computer. The Kunert patent teachings found from Col. 1, lines 26-36 teach that a PCMCIA card may include an RF transponder. Kunert does not teach, however, that the RF transponder or PCMCIA card includes means for storing an antenna history bit indicating that an RF antenna, or the RF transponder, was once attached to the computer.

Applicants respectfully assert that, since none of the Isikoff, Elledge, or Kunert patents teaches an RFID chip and storage means or steps for storing data comprising at least an antenna history bit about original attachment of an RR antenna security device, storing data comprising the antenna history bit without powering on the computer, accessing the stored antenna bit data and determining if a security device has been removed based on accessing that data, and

determining if removal was authorized, with storage of authorized removal data, it cannot be maintained that the combination of references obviates the invention as claimed.

The Court of Appeals for the Federal Circuit has clearly stated that, for a *prima facie* case of obviousness, the prior art must teach or suggest all of the claim features *(In re Wilson*, 424 F. 2d 1382, 1385, 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970)). Since the cited patents do not teach or suggest storing an antenna history bit about original attachment of an RF antenna security device, storing data comprising the antenna history bit without powering on the computer, accessing the stored antenna bit data and determining if a security device has been removed based on accessing that data, and determining if removal was authorized, with storage of authorized removal data, it cannot be maintained that the combination of references obviates the invention as claimed. Accordingly, Applicants respectfully request reconsideration of the rejection of the claims as unpatentable over the combined teachings of Isikoff, Elledge and Kunert.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

J. Tanaka, et al

By: Anne Vachon Dougherty

Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910